# MATH 314 Spring 2018 - Class Notes 

$2 / 21 / 18$
Scribe: Tyler Schmitz
Summary: The use of Euler's Phi Function (Totient Function)

## Notes:

$\phi(n)$ is equivalent to the number of residues mod n that are coprime to n An example is $\phi(26)=12$ (odd numbers and not 13 ).

If the number n is prime $(\mathrm{p})$ then we take $\phi=p-1$. For example $\phi(7)=6$.

## Product of 2 primes:

For $\phi(p q)$ where p and q are both primes, we use the Chinese Remainder Theorem
$x=(-)(\bmod p)$
$x=(-)(\bmod q)$
How many things can go into each equation?
$\mathrm{p}-1$ and $\mathrm{q}-1$ respectively
$\phi(p q)=(p-1)(q-1)=p q(1-(1 / p))(1-(1 / q))$
Example- $\phi(26)=\phi(2 * 13)=26(1-1 / 13)(1-1 / 2)=12$
The 12 coprime numbers are $1,3,5,7,9,11,15,17,19,21,23,25$
And not $2,4,6,8,10,12,13,14,16,18,20,22,24,26$
$\Pi$ is used like Sigma for multiplication instead of addition.

$$
\phi(n)=n \prod_{p \mid n}\left(1-\frac{1}{p}\right)
$$

In this notation for every prime that divides n , there is another term added A second example:
ex: $\phi(100)=100 \Pi(1-1 / p)$
$\phi(100)=100 \Pi(1-1 / p)$
The 2 prime factors of 100 are 2 and 5 so we have 2 terms. If there were more prime factors we would include these as well.

So:

$$
\begin{aligned}
& \phi(100)=100 \Pi(1-1 / 2)(1-1 / 5) \\
& =100(1 / 2)(4 / 5) \\
& =50(4 / 5) \\
& =40
\end{aligned}
$$

ex2: The prime factors of 429 are $3,11,13$

$$
\begin{aligned}
& \phi(429)=429 \Pi(1-1 / 3)(1-1 / 11)(1-1 / 13) \\
& =429(2 / 3)(10 / 11)(12 / 13) \\
& =286(10 / 11)(12 / 13) \\
& =260(12 / 13) \\
& =240
\end{aligned}
$$

So there are 240 numbers coprime to 429

## Euler's Theorem

If a and n are coprime then $a^{\phi(n)}=1(\bmod n)$. ex: Let $a=3$ and $n=4$.
$\phi(n)=\phi(4)=4(1-(1 / 2))=2$.
Euler's Theorem says that $3^{\phi(4)}=9=1(\bmod 4)$.
Note: that if $n=p$ is prime then Fermat's Little Theorem is a special case of Euler's Theorem.

The General Principle for modular arithmetic with exponents is if we work $\bmod (\mathrm{n})$ then in the exponents we work mod $\operatorname{Phi}(\mathrm{n})$.

## 3-Pass Protocol

- Suppose Alice and Bob want to send package via UPS but Eve opens package through the email
- Alice and Bob have padlocks but they don't have the same keys
- Alice takes package and locks it with her key and sends it to Bob
- Bob locks it again with his padlock and sends it back to Alice
- Alice sends the box back to Bob after removing her lock
- Then Bob unlocks the box and reads the message because only his lock was still in the box


## 3-Pass Protocol Mathematically

We want to encode our message as a number m .
We need to pick a large prime number p, p isn't secret and Eve can know it.
Aice's key is a number coprime to ( $\mathrm{p}-1$ ), call it "a", and Bob's key "b" is kept secret and is also coprime to ( $\mathrm{p}-1$ ).

Both are kept secret, Alice only knows hers and Bob only knows his.
Alice's Encryption Function is $E_{A}(m)=m^{a}(\bmod p)$.
Bob's Encryption function is $E_{B}(m)=m^{b}(\bmod p)$.
To decrypt Alice needs to undo raising something to the "a" power mod p.
Alice will compute $a^{-1}(\bmod p-1)$
Bob will compute $b^{-1}(\bmod p-1)$

Note: that if Alice encrypts $m$ she gets $m^{a}(\bmod p)$
Now if she raises this to the $a^{-1}(\bmod p-1)$ then

$$
\begin{aligned}
& m^{a^{a^{-1}}}(\bmod p)=m^{a a^{-1}}=m^{k(p-1)^{-1}}(\bmod p) \\
&=m^{(p-1)^{k}}(\bmod p)
\end{aligned}
$$

This is Fermat's Theorem.

## The Whole process is:

- Alice's Encryption function is $E_{A}(m)=C_{1}=m^{a}(\bmod p)$
- Sends $C_{1}$ to Bob
- Bob's Encryption function is $E_{B}\left(C_{1}\right)=C_{2}=C_{1}^{b}(\bmod p)$
- Sends C2 to Alice
- Alice's Decryption function is $D_{A}\left(C_{2}\right)=C_{3}=C_{2}^{a^{-1}}(\bmod p)$
- Bob's Decryption function is $D_{B}\left(C_{3}\right)=C_{4}=C_{3}^{b^{-1}}(\bmod p)$

